Revista Iberoamericana para la Investigación y el Desarrollo Educativo
ISSN 2007 - 7467

https://doi.org/10.23913/ride.v15i29.2098

Artículos científicos

Ciberviolencia perpetrada por estudiantes de secundaria a docentes de Sinaloa, México: percepción, incidencia y estrategias de afrontamiento

Cyberviolence perpetrated by secondary school students Against Teachers in Sinaloa, Mexico: Perception, Incidence, and Coping Strategies

Violência cibernética perpetrada por estudantes do ensino médio contra professores em Sinaloa, México: percepção, incidência e estratégias de enfrentamento

María Luisa Pereira Hernández
Universidad Pedagógica del Estado de Sinaloa, México
pereirahdz@hotmail.com
https://orcid.org/0000-0002-4748-5397

Resumen

El estudio se enfoca en analizar la incidencia y las características de la ciberviolencia hacia los docentes en el estado de Sinaloa, México. Se empleó una metodología cuantitativa de alcance exploratorio descriptivo para obtener una comprensión integral del fenómeno. Se aplicó una encuesta validada por jueces de 33 preguntas a 852 docentes de secundarias estatales, del Estado de Sinaloa. Los resultados revelaron ciberataques y ciberbullying hacia los docentes, el 77% informó conocer a compañeros y el 16.9% compañeras víctimas, se identificaron diversas estrategias de afrontamiento utilizadas por los afectados, incluyendo el diálogo con el estudiantado (45) y la comunicación con las autoridades escolares (22). Los hallazgos destacan la necesidad de una mayor conciencia y capacitación sobre ciberseguridad en el ámbito educativo, así como de políticas efectivas para abordar el ciberbullying. Las conclusiones principales subrayan la importancia de promover una cultura de seguridad cibernética en las escuelas y de implementar intervenciones específicas para prevenir y mitigar la ciberviolencia del estudiantado al docente.

Palabras clave: ciberbullying, ciberacoso, formación de docentes, ciberseguridad, tecnología educativa.

Abstract

The study focuses on analyzing the incidence and characteristics of cyberviolence towards teachers in the state of Sinaloa, Mexico. A quantitative methodology with an exploratory descriptive scope was used to obtain a comprehensive understanding of the phenomenon. A 33-question survey, validated by experts, was applied to 852 secondary school teachers in Sinaloa. The results revealed cyberattacks and cyberbullying towards teachers, with 77% reporting knowing colleagues who were victims and 16.9% reporting knowing female colleagues who were victims. Various coping strategies used by the affected teachers were identified, including dialogue with students (45) and communication with school authorities (22). The findings highlight the need for greater awareness and training on cybersecurity in the educational field, as well as effective policies to address cyberbullying. The main conclusions emphasize the importance of promoting a culture of cybersecurity in schools and implementing specific interventions to prevent and mitigate student-to-teacher cyberviolence.

Keywords: cyberbullying, cyberharassment, teacher training, cybersecurity, technology education.

Resumo

O estudo se concentra em analisar a incidência e as características da ciberviolência contra professores no estado de Sinaloa, México. Utilizou-se uma metodologia quantitativa de escopo exploratório descritivo para obter uma compreensão abrangente do fenômeno. Uma pesquisa validada por juízes com 33 perguntas foi aplicada a 852 professores do ensino médio estadual do Estado de Sinaloa. Os resultados revelaram ataques cibernéticos e cyberbullying contra professores, 77% relataram conhecer colegas de classe e 16,9% outras vítimas, foram identificadas várias estratégias de enfrentamento utilizadas pelas pessoas afetadas, incluindo o diálogo com os alunos (45) e a comunicação com as autoridades (22). As conclusões destacam a necessidade de uma maior sensibilização e formação em segurança cibernética na educação, bem como de políticas eficazes para combater o cyberbullying. As principais conclusões destacam a importância de promover uma cultura de cibersegurança nas escolas

e de implementar intervenções específicas para prevenir e mitigar a ciberviolência dos alunos aos professores.

Palavras-chave: cyberbullying, cyberbullying, formação de professores, cibersegurança, tecnologia educacional.

Fecha Recepción: Abril 2024 **Fecha Aceptación:** Septiembre 2024

Introducción

La creciente penetración de la tecnología digital en la vida cotidiana ha traído consigo una serie de desafíos y amenazas, destacando entre ellas el fenómeno de los ciberataques. En México, como en muchos otros países, el ciberacoso representa una preocupación cada vez más acuciante, con repercusiones significativas en la seguridad y el bienestar de la población, especialmente entre los jóvenes y las mujeres.

En este contexto, los docentes no han sido inmunes a estas formas de violencia digital, enfrentándose a ciberataques perpetrados por estudiantes, padres de familia y colegas (Challenor, 2019; De Wet, 2010; González, 2024; Huang *et al.,* 2014; Kauppi y Pörhölä, 2012a; Kauppi y Pörhölä, 2012b; Kopecký y Szotkowski, 2017, Mooij, 2011; Pereira, 2021; Pereira, 2023; Pereira, 2024; Tolentino, 2016). Sin embargo, la falta de datos y el bajo índice de denuncias han dificultado la comprensión completa de este fenómeno y la implementación de medidas adecuadas de prevención y protección. En este sentido, surge la necesidad de investigar el comportamiento de datos relacionados con los ciberataques enfrentados por los docentes del estado de Sinaloa, con el fin de entender mejor la naturaleza y la magnitud de este problema, así como para diseñar estrategias efectivas de intervención.

En 2019, más del 25% de los mexicanos entre 12 y 19 años fueron víctimas de ciberacoso. Este fenómeno afecta especialmente a las mujeres en este grupo de edad, con un 28% de ellas experimentando diversas formas de acoso cibernético, que incluyen llamadas, mensajes, contenido multimedia, robo de identidad y publicación de información personal. Un dato alarmante es que el 80% de las víctimas declararon no conocer la identidad de sus acosadores, lo que subraya la complejidad y el anonimato que caracteriza al ciberacoso en la era digital. Este aumento en los casos de ciberacoso resalta la necesidad urgente de abordar este problema y de implementar medidas efectivas para proteger a los jóvenes en línea (Instituto del Derecho de las Telecomunicaciones [IDET], 2020).

Durante los primeros nueve meses de 2020, México fue el país más atacado en Latinoamérica, recibiendo más del 22% de los ataques de ransomware en la región, lo que

afectó a casi 300 mil empresas. También señala que, en 2017, un número significativo de mexicanos fueron víctimas de cibercrimen, con un impacto económico de miles de millones de dólares (IDET, 2020).

El aumento de la ciberdelincuencia ha impactado significativamente a México, con un incremento notable en ataques a infraestructuras críticas, fraudes, suplantación de identidad y ataques de ransomware. Entre septiembre y octubre de 2020, se registraron más de 10 mil ciberataques, gracias a la rápida adopción de nuevas tecnologías, como inteligencia artificial y big data, que han potenciado las capacidades de los agresores cibernéticos, afectando tanto a ciudadanos como a instituciones públicas y privadas. Las repercusiones económicas y sociales son evidentes, en empresas mexicanas que han enfrentado pérdidas millonarias, debido a los ataques de ransomware y un crecimiento alarmante de la victimización por cibercrimen, especialmente entre los jóvenes, siendo así una necesidad imperativa, repensar las estrategias de seguridad nacional y ciberseguridad en este contexto de transformación digital acelerada (IDET, 2020).

Existen datos alarmantes sobre el panorama de la ciberseguridad en México, durante el año 2021, México experimentó 156 mil millones de amenazas de ciberataques y el fraude cibernético ascendió a ocho mil millones de dólares anuales, de igual manera se revela un aumento del 600% en los intentos de ciberataques en América Latina y el Caribe durante 2021 (IDET, 2022).

En el panorama actual de las amenazas cibernéticas, se destaca un aumento significativo del 28% en los ciberataques durante 2022 en comparación con el año anterior, además se anticipa que estas amenazas evolucionarán y se volverán más sofisticadas durante el año 2023, afectando a empresas, administraciones y usuarios; ante esta alza se logran identificar seis tipos principales de ciberataques, incluyendo malware avanzado, ransomware más sofisticado, phishing y smishing mejorados, técnicas de intrusión a través de redes domésticas debido al aumento del teletrabajo, el uso de inteligencia artificial para métodos de intrusión y deepfakes, que representan mensajes engañosos creados con inteligencia artificial (IDET, 2022a).

De acuerdo a un estudio de seguridad de Unisys basado en encuestas nacionales e internacionales realizadas a 11 mil adultos de 18 a 64 años en 11 mercados diferentes se reveló que el robo de identidad y el fraude de tarjetas bancarias son las principales preocupaciones de los mexicanos en temas de ciberseguridad, a pesar de que el 66% de los encuestados manifestó desconfianza al hacer clic en enlaces sospechosos, solo el 29% estaba familiarizado con estafas más sofisticadas como el secuestro SIM, y apenas el 22% conocía

las organizaciones adecuadas para denunciar ciberataques; en respuesta a estos desafíos, se destacó la necesidad de adoptar datos biométricos para mejorar la seguridad de los usuarios y prevenir ataques o filtraciones de datos (IDET, 2021).

Los datos manifiestan un alza en relación al género. El ciberacoso en México es un fenómeno preocupante que afecta a una parte significativa de la población, especialmente a mujeres y niñas, donde 95 de cada 100 víctimas de violencia digital son mujeres y ocho de cada 10 personas agresoras se les identifica como hombres.

De acuerdo con las cifras recopiladas, durante el año 2022, aproximadamente 9.8 millones de mujeres mayores de 12 años fueron víctimas de ciberacoso, en comparación con 7.6 millones de hombres en la misma categoría demográfica; los incidentes son especialmente frecuentes entre las mujeres jóvenes de 20 a 29 años, donde el 29.3% reportó haber sido víctima en los últimos 12 meses, se destaca también que la mayoría de los actos son perpetrados por desconocidos, representando el 61.3% de los casos, mientras que el 19.1% fue cometido por conocidos; además, las plataformas digitales más utilizadas, como Facebook y WhatsApp, son los medios principales a través de los cuales se produce el ciberacoso, constituyendo el 44.5% y el 45.5% de los casos, respectivamente (Hernández, 2022). De acuerdo a las cifras proporcionadas, el ciberacoso representa una grave amenaza para la seguridad y bienestar de las personas en México, con un impacto desproporcionado en mujeres y niñas.

El fenómeno de la violencia ha llegado a las escuelas. Se informa que hasta el 60% de los maestros de escuelas primarias y secundarias en México han sido víctimas de violencia por parte de estudiantes, según el Dr. José Carlos Hernández, especialista en Sistemas Penales y Política Criminal, quien destaca que solo el 17% de los docentes afectados se atreve a presentar una queja formal ante alguna autoridad, principalmente debido al temor a represalias por parte de los padres del alumnado o a perder su plaza; se atribuye el aumento de la violencia a factores como la falta de políticas públicas coherentes en educación y la violencia prevaleciente en los entornos familiares de los estudiantes, además se enfatiza la necesidad urgente de incorporar la Axiología y los Derechos Humanos en todo el sistema educativo para abordar el problema y restaurar el tejido social (González, 2024).

Aunque la violencia física y verbal al docente recibe actualmente mayor atención, debido a su visibilidad y capacidad de manifestarse en la interacción presencial, es considerable destacar que los docentes también son objeto de ciberataques por parte de estudiantes, padres de familia y colegas, aunque existen pocos datos al respecto. El hecho de que los porcentajes de denuncia ante actos de violencia hacia el docente sean bajos, refleja

una tendencia aún más marcada en el caso de los ciberataques, exacerbada por el desconocimiento del agresor y de los protocolos a seguir en tales situaciones.

En un estudio realizado con 162 docentes encuestados, se encontró sorprendente, que solo un 16.8% admitió haber sido víctima de algún tipo de ciberagresión, siendo los teléfonos celulares inteligentes y las tabletas los dispositivos más comunes utilizados para llevar a cabo estos ataques; Facebook fue identificado como la plataforma más frecuentemente utilizada para perpetrar ciberataques, con un 86% de los casos registrados (Pereira, 2021).

Entre los ciberataques realizados a docentes, el compartir material degradante se identificó como el tipo más prevalente, seguido por el ciberbaiting "provocar al docente y grabar su reacción sorprendida, principalmente a través de teléfonos móviles, y posteriormente compartir estos materiales" (Kopecký y Szotkowski, 2017, p. 2) y las amenazas de intimidación o extorsión; una tendencia preocupante observada en el estudio fue la falta de abordaje del problema por parte de los docentes, con un alarmante 86% que optó por no confrontar la situación, mientras que solo un 13% decidió abordar directamente el problema con el grupo; los resultados revocan la urgencia de implementar medidas efectivas para proteger a los docentes y fomentar un entorno escolar seguro y respetuoso frente a la ciberviolencia (Pereira, 2021).

Las definiciones de ciberbullying son amplias y diversas, lo que dificulta identificar cuándo se trata de una agresión única o de uno que cumpla con los criterios de repetición, duración y percepción de daño por parte de la víctima, así como la presencia de un desequilibrio de poder entre el agresor y la víctima.

La conceptualización se fundamenta en las definiciones existentes de bullying tradicional, que se percibe como actos o comportamientos agresivos, intencionales y repetidos realizados contra un individuo o grupo que no puede defenderse fácilmente. Olweus (1993) advierte sobre la necesidad de distinguir entre bullying y agresión, donde la agresión se percibe como un evento único, mientras que el bullying es un fenómeno repetido, caracterizado precisamente por el desequilibrio de poder entre el agresor y la víctima (Olweus, 1993; Whitney y Smith, 1993; Rigby, 1997; Smith y Sharp, 1994). Se puede decir entonces que el término ciberbullying sigue lógicamente la definición de bullying tradicional y la extiende con especificidades adicionales, especialmente en relación con las tecnologías de la información y la comunicación (TIC).

Existe una multiplicidad de definiciones de ciberbullying, que en muchos casos no son compatibles entre sí. Algunos autores lo consideran como cualquier ataque relacionado con hacer daño a otros en el entorno de Internet, mientras que otros señalan que el "verdadero

cyberbullying" debe ser deliberado, repetido e intenso (Juvonen y Gross, 2008; Patchin y Hinduja, 2006).

Entre las definiciones más utilizadas se encuentran la que lo define como una actividad deliberada, repetida y perjudicial utilizando computadoras, teléfonos móviles y otros dispositivos electrónicos (Hinduja y Patchin, 2008; Patchin y Hinduja, 2006). De igual manera el cyberbullying puede entenderse como cualquier acción llevada a cabo en el ciberespacio con la intención de insultar o humillar a otros, mientras que otros lo definen como daño intencional y repetido causado por medios o textos electrónicos (Juvonen y Gross, 2008; Hinduja y Patchin, 2008). Es una forma de comportamiento de acoso, se manifiesta cuando se utilizan diversas redes sociales como Facebook y Twitter para comunicaciones abiertas, y puede ser impuesto deliberadamente a alguien con el fin de dañar o acosar (Huang *et al.,* 2014).

En otros aspectos, algunas definiciones retoman el uso de diferentes medios y tecnologías, como correo electrónico, mensajes de texto, llamadas telefónicas, sitios web y aplicaciones de mensajería y redes sociales, con la intención de hostigar, amenazar, humillar o atacar a otras personas, especialmente adolescentes (Li, 2007; Slonje y Smith, 2008; Dehue *et al.,* 2009; Smith *et al.,* 2008; Kowalski *et al.,* 2012). Se experimenta a través de correos electrónicos, mensajes en vivo y comunicaciones, sitios web y juegos en línea, así como mensajes o imágenes enviadas a teléfonos móviles (Kowalski *et al.,* 2012).

Las diversas definiciones de ciberbullying reflejan la complejidad y la amplitud del fenómeno, así como la evolución constante de las formas en que se manifiesta en el entorno digital. Aunque todas las definiciones coinciden en la implicación de un comportamiento agresivo, intencional y repetido utilizando tecnologías de la información y la comunicación, existe una falta de consenso sobre la especificidad de sus características y la gravedad de sus efectos. Además, la identificación precisa puede resultar difícil debido a su naturaleza variable y a las múltiples formas en que puede manifestarse en línea.

Bajo estas premisas, surge la siguiente pregunta de investigación ¿Cuál es la incidencia de ciberviolencia del estudiante al docente de secundaria, en el estado de Sinaloa, México? ¿Cuáles son las estrategias de afrontamiento utilizadas por los docentes en respuesta a esta problemática? ¿Cuál es la prevalencia de los ciberataques por parte del estudiantado que enfrentan los docentes? y ¿Quiénes fueron los ciberatacantes? Las preguntas buscan entender la naturaleza y la incidencia del fenómeno, así como las tendencias y patrones que puedan surgir de los datos recopilados. Por ende, los siguientes objetivos de investigación se derivaban de las preguntas mencionadas: determinar la incidencia de ciberviolencia;

identificar las estrategias de afrontamiento utilizadas; determinar la prevalencia de los ciberataques enfrentados e identificar a los perpetradores de los ciberataques dirigidos a los docentes de secundaria en el estado de Sinaloa, México.

Ciberbyllying al docente

Los docentes pueden llegar a ser víctimas de acoso a través de declaraciones maliciosas publicadas en redes sociales (Tolentino, 2016). Estas prácticas en plataformas digitales a menudo incluyen insultos relacionados con la inteligencia, características físicas y valores de las víctimas (Hua *et al.,* 2019; Zhao *et al.,* 2016). Por ejemplo, se pueden utilizar palabras que retraten a alguien como incompetente, imprudente o carente de inteligencia para insultar su inteligencia. Además, pueden compartirse imágenes de "*body-shaming*" que se burlan de las características físicas de la víctima, como el color de piel oscuro o arrugas en la cara y ahora elaboradas con mucha más facilidad con el uso de la inteligencia artificial.

El acoso electrónico experimentado por los maestros abarca una variedad de formas, desde la publicación de imágenes y clips audiovisuales obscenos y editados en páginas de Facebook falsas, hasta la difusión de comentarios abusivos, hirientes y embarazosos en su contra, el hackeo de sus cuentas de correo electrónico y la propagación de virus, así como la diseminación de comentarios ofensivos a través de correos electrónicos, mensajes de texto, salas de chat o páginas web (Eden *et al.,* 2013; Garrett, 2014; Kauppi y Pörhölä, 2012a; Tolentino, 2016). Además de estas formas de acoso en línea, los maestros también son objeto de acoso físico, verbal y no verbal, así como de acoso indirecto (James *et al.,* 2008; Kauppi y Pörhölä, 2012b; Mooij, 2011). Se señala que la incapacidad de los maestros para manejar y disciplinar a los estudiantes, así como su comportamiento estricto y las calificaciones bajas que otorgan, son causas importantes de ser acosados por los estudiantes (De Wet, 2010). Asimismo, los acosos sexuales de los estudiantes universitarios hacia profesoras jóvenes, las amenazas y las difamaciones en las redes sociales que viven día a día los docentes, son temas de investigación que plantean preocupaciones adicionales en relación con el acoso hacia los maestros.

Metodología

Para este estudio se consideró pertinente la metodología de investigación cuantitativa con alcance exploratorio, dado a que el análisis estadístico de los datos puede ofrecer una comprensión objetiva de la naturaleza y la magnitud del problema de la ciberviolencia hacia los docentes en Sinaloa. Estas cifras brindan una base sólida para informar el desarrollo de políticas y estrategias de prevención y respuesta efectivas.

Con base en lo anterior se retoma que la investigación cuantitativa explica fenómenos mediante la recopilación de datos numéricos detallados e invariables que se analizan utilizando métodos basados en matemáticas, en particular estadísticas, que plantean preguntas sobre quién, qué, cuándo, dónde, cuánto, cuántos y cómo. Trata en números, lógica y una postura objetiva (Mohaja, 2020).

En cuanto al alcance, la investigación es exploratoria y descriptiva, como su nombre indica, tiene la intención de simplemente explorar las preguntas de investigación y no pretende ofrecer soluciones finales y concluyentes a problemas existentes, este tipo de investigación suele llevarse a cabo para estudiar un problema que aún no ha sido claramente definido, es realizada con el fin de determinar la naturaleza del problema (Dudovskiy, 2022).

Es también de alcance descriptivo, dado que se parte del entendimiento previo de las características del fenómeno en cuestión como se realizó en Pereira, (2021), centrándose ahora, en la exposición y descripción de los aspectos presentes en un grupo específico de individuos, como lo son los docentes del Estado de Sinaloa. En el contexto de investigaciones descriptivas cuantitativas, se emplean análisis de datos estadísticos para examinar tendencias centrales y variabilidad. Aunque en este tipo de investigación es posible plantear hipótesis que busquen caracterizar el fenómeno estudiado, no son consideradas como un requisito indispensable (Ramos, 2020).

Como técnica de investigación se utilizó una encuesta. Pinsonneault y Kraemer (1993, como se citó en Glasow, 2005) definieron una encuesta como un "medio para recopilar información sobre las características, acciones u opiniones de un gran grupo de personas" (p. 77). Las encuestas también pueden utilizarse para evaluar las necesidades, demandas y examinar el impacto (Salant y Dillman, 1994, p. 2, como se citó en Glasow, 2005). Dicho instrumento fue validado a partir de la técnica de validación de jueces.

De acuerdo con Corral (2009), la validación implica que un instrumento debe capturar de manera precisa y representativa un dominio específico del contenido de la característica o rasgo que se está evaluando, es decir, busca determinar en qué medida los ítems o preguntas

de un instrumento reflejan adecuadamente el universo de contenido relacionado con la característica o rasgo en cuestión y con respecto a la confiabilidad, se refiere al grado de precisión y exactitud en el proceso de medición.

La aprobación del contenido, gracias al informe de expertos, se llevó a cabo de manera metódica y esclarecedora, logrando un consenso entre los jueces. La encuesta utilizada en esta investigación abordó cinco variables significativas: datos sociodemográficos, capacitación, seguridad en Internet, ciberviolencia dirigida por estudiantes hacia los docentes a nivel personal y como observador, y estrategias de afrontamiento; el instrumento constaba de 33 preguntas distribuidas en estos cinco factores. Una vez completado el trabajo, la prueba F de Friedman demostró ser útil para confirmar los informes en relación con la investigación de un grupo de individuos (González y Pereira, 2023)

En Sinaloa se tiene una población total de 13,258 docentes de secundaria, de los cuales 7,402 pertenecen a escuelas secundarias estatales. Las escuelas estatales se dividen en públicas y privadas, siendo 5,725 docentes de escuelas públicas y 1,677 de escuelas privadas en el estado de Sinaloa (Instituto Nacional de Estadística y Geografía [INEGI], 2023).

Para determinar el tamaño de una muestra válida, fue necesario considerar varios factores, incluyendo el tamaño de la muestra en relación con el tamaño de la población total y la técnica de muestreo utilizada. En este caso, se tiene una población total de 7,402 docentes y una muestra de 961. Para evaluar la validez de la muestra, se calculó el error muestral utilizando la fórmula: $E = \frac{\frac{z\sqrt{p(1-p)}}{N}}{\sqrt{n}}$

Por lo tanto, el error muestral es aproximadamente 0.000336 lo que significa que el margen de error para la muestra es muy pequeño en comparación con el tamaño de la población. Se puede decir entonces que, con un nivel de confianza del 95%, la muestra de 961 docentes es válida para representar la población total de 7 402 docentes.

De la muestra obtenida de 961 docentes de secundarias estatales del Estado de Sinaloa, se obtuvo la distribución por tipo de escuela 852 (88.7%) correspondían a escuelas públicas y 109 (11.3%) de escuelas privadas y en cuanto a la distribución por género, la muestra tiene una mayor proporción de mujeres 544 (56.7%) que de hombres 414 (43.2%).

En cuanto a la distribución de los docentes encuestados en grupos de edad se obtuvo lo siguiente, 135 (14%) tienen entre 20 y 30 años, 384 (40%) tienen entre 31 y 40 años, 299 (31.1%) tienen entre 41 y 50 años, 133 (13.8%) tienen entre 51 y 60 años y 13 (1.4%) tienen más de 61 años.

En relación a los años de servicio la muestra se encontró que 236 (24.6%) cuentan de cero a cinco años, 279 (29%) de seis a 10 años, 259 (27%) de 11 a 20 años, 159 (16.5) de 21 a 30 años, 30 (3.1%) de 31 a 40 años, tres (0.3%) de 41 a 50 años y uno (0.1%) de entre 51 y 60 años.

En lo que respecta al grado de estudio se obtuvo que 648 (67.6%) cuenta con título de Licenciatura, 84 (8.8%) son pasantes de Licenciatura, 80 (8.3%) son titulados de Maestría, 97 (10.1%) pasantes de Maestría, 13 (1.4%) son titulados de Doctorado, 23 (2.4%) pasantes de Doctorado y 14 (1.5%) solo cuentan con preparatoria.

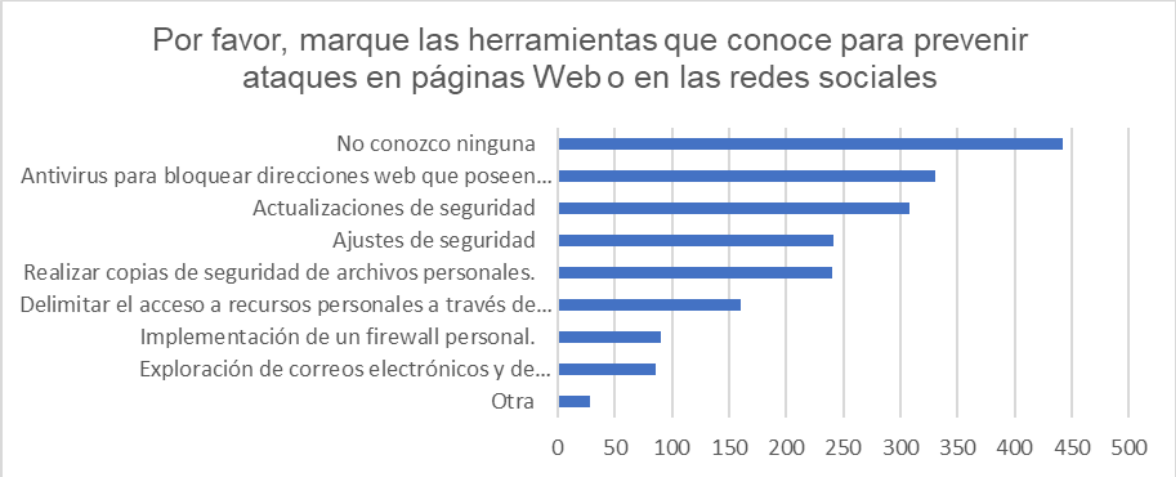
En relación a la muestra existe una predominancia de docentes trabajando en escuelas públicas, una mayor proporción de mujeres que de hombres, una distribución amplia pero concentrada por edades en la etapa media de la carrera docente, y una mezcla de experiencia y relativa novedad en términos de años de servicio, además la mayoría de los docentes cuentan con al menos un título de Maestría, lo que sugiere un nivel educativo relativamente alto.

El escenario, el estado de Sinaloa, según la Dirección General de Planeación, Programación y Estadística Educativa de la Secretaría de Educación Pública (DGPPYEE-SEP, 2023) cuenta con una extensión territorial de 57,365 km² y una población de 3,026,943 habitantes, representa aproximadamente el 2.9% del territorio nacional y el 2.4% de la población total del país; la población sinaloense tiene una distribución de género equilibrada, con un 50.6% de mujeres y un 49.4% de hombres; en cuanto a la educación, para el ciclo escolar 2021-2022, Sinaloa contó con una matrícula total de 869,881 estudiantes, de los cuales el 50.8% son mujeres y el 49.2% son hombres. Esta matrícula representa aproximadamente el 2.5% del total del Sistema Educativo Nacional. La distribución de la matrícula por tipo educativo muestra que el 69.6% corresponde a educación básica, el 15.6% a educación media superior y el 14.7% a educación superior. En cuanto a la cobertura educativa, se observa que en educación preescolar la cobertura es del 70.4%, con una atención por grupo de edad que varía entre el 52.8% y el 90.9%. En educación primaria, la cobertura alcanza el 97.9%, con una tasa neta de escolarización del 92.4% y un abandono escolar del -0.1%. Por su parte, en educación secundaria la cobertura es del 94.9%, con un abandono escolar del 3.0%.

Análisis de resultados

En un primer instante se recuperan los resultados relacionados a las medidas de seguridad, dando énfasis en las actualizaciones de seguridad y el uso de antivirus. Sin embargo, también resalta la necesidad de aumentar la conciencia sobre otras medidas preventivas, como la exploración de correos electrónicos, la delimitación del acceso en dispositivos móviles y la implementación de firewalls personales, como se destaca a continuación en la figura 1.

Figura 1. Herramientas de ciberseguridad.



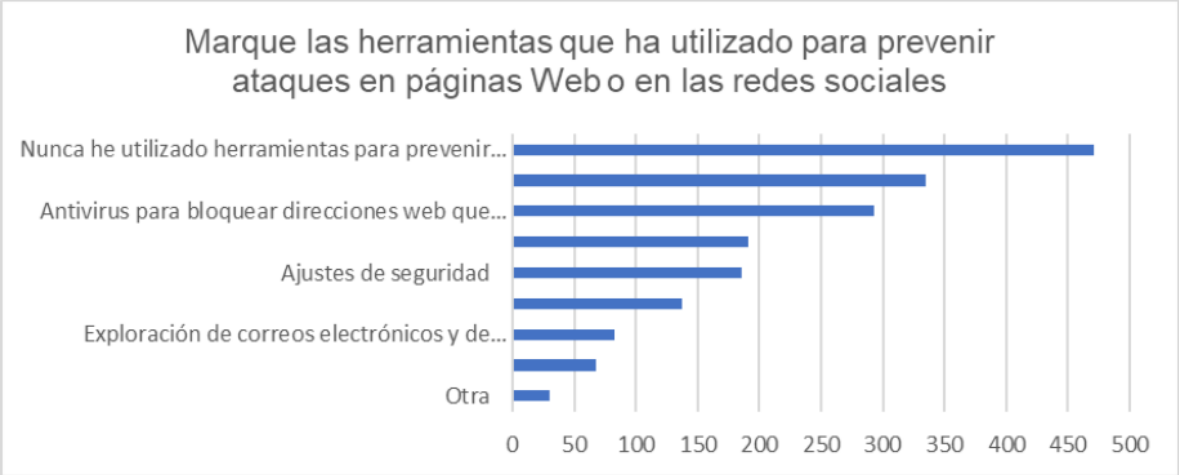
Fuente: Elaboración propia.

En cuanto al nivel de conciencia sobre seguridad y el hecho de que el 46% de los encuestados indican no conocer ninguna herramienta específica para prevenir ataques en páginas web o redes sociales, sugiere un nivel preocupante de falta de conciencia sobre seguridad cibernética, además destaca la necesidad de educación y concienciación sobre la importancia de la seguridad en línea. No obstante, en cuanto a la prevalencia de herramientas de seguridad las respuestas indican su prevalencia y reconocimiento como medidas efectivas de prevención, reflejando una comprensión básica de las prácticas de seguridad en línea. De igual manera, los aspectos adicionales resaltan la importancia de promover una cultura de seguridad cibernética más amplia y diversificada, así como de educar a los docentes sobre la importancia de adoptar medidas proactivas para proteger su seguridad y privacidad en línea, cabe aclarar que las respuestas de "otra" se identificaron en actividades relacionadas a ajustes de seguridad.

Los resultados muestran una variedad de medidas de seguridad utilizadas por los encuestados, con un énfasis en las actualizaciones de seguridad y el uso de antivirus. Sin

embargo, también resalta la necesidad de aumentar la conciencia sobre otras medidas preventivas, como la exploración de correos electrónicos y la delimitación del acceso en dispositivos móviles. Las respuestas obtenidas en la pregunta relacionada a las herramientas utilizadas para prevenir ataques en la Web o en redes sociales, marcan también una alarmante relación en cuanto al por qué se viven ataques de ciberviolencia, como se observa en la Figura 2.

Figura 2. Herramientas usadas por los docentes para prevenir ciberataques.



Fuente: Elaboración Propia.

La falta de conocimiento sobre herramientas de seguridad en línea (46% de los encuestados) contribuye a la vulnerabilidad de las personas ante ataques de ciberviolencia. La falta de conciencia sobre cómo protegerse en línea, expone a los individuos a riesgos de violencia en línea, por lo que se requiere el docente una capacitación constante sobre ciberseguridad.

La relación entre los datos sobre las herramientas que los encuestados conocen y las herramientas que realmente utilizan puede proporcionar información sobre la conciencia, la adopción y la efectividad de las medidas de seguridad en línea. Podría haber una correlación positiva entre el conocimiento y el uso de herramientas de seguridad en línea. Es decir, es probable que los encuestados que conocen una amplia gama de herramientas de seguridad también sean más propensos a utilizarlas en comparación con aquellos que conocen menos herramientas.

Por otro lado, también es posible que exista una correlación negativa entre el conocimiento y el uso de herramientas de seguridad. Los encuestados pueden estar familiarizados con una variedad de herramientas de seguridad, pero pueden optar por no utilizarlas por diversas razones, como la complejidad de la configuración, la falta de confianza en su efectividad o simplemente la falta de interés en la seguridad en línea.

Además, es posible que los encuestados estén familiarizados con una amplia gama de herramientas de seguridad, pero solo utilicen un subconjunto de ellas o simplemente podrían estar utilizando un software antivirus sin comprender completamente cómo funciona o qué otras medidas de seguridad están disponibles. Lo necesario a rescatar es el hecho de que, casi la mitad de los encuestados (46%) afirman no conocer ninguna herramienta específica para prevenir ataques en línea, lo cual es preocupante, sugiriendo de nueva cuenta una falta de conciencia o educación sobre las medidas de seguridad disponibles, lo que podría dejar a estos individuos más vulnerables a los ataques cibernéticos.

Los datos obtenidos cuando se les cuestionó si alguna vez habían sido víctimas de ciberataques o ciberbullying por algún estudiante o grupos de estudiantes de su centro de trabajo, revelan algunas tendencias y percepciones interesantes sobre la incidencia de ciberataques educativos, tanto desde la perspectiva de los docentes como desde la percepción de casos relacionados con el estudiantado hacia los docentes, se tiene que, 788 (82%) respondieron que no, 99 (10.3%) que no estaban seguros y 74 (7.7%) contestaron que sí conocían casos; no obstante, cuando se les cuestionó si habían conocido algún caso de ciberataque o ciberbullying del estudiantado al docente los porcentajes aumentaron: 274 (28.5%) contestaron que sí conocían casos, 93 (9.7%) que no estaban seguros y 594 (61.8%) que no conocían casos.

En razón a la autoexperiencia, el hecho de que el 82% de los docentes encuestados respondieran que nunca habían sido víctimas de ciberataques o ciberbullying por parte de estudiantes es un hallazgo positivo en términos de la percepción de seguridad en el lugar de trabajo. Sin embargo, es importante considerar que un pequeño porcentaje (7.7%) sí reportó haber sido víctima, lo que indica que estos problemas existen en entornos educativos.

En el tema de conocimiento de casos, el aumento significativo en el porcentaje de docentes que informaron conocer casos de ciberataques o ciberbullying del estudiantado hacia los docentes (28.5%) es notable, rescatando que, si bien es posible que ciertos docentes no hayan experimentado personalmente estos ataques, son conscientes de que estos problemas pueden estar ocurriendo en su entorno laboral.

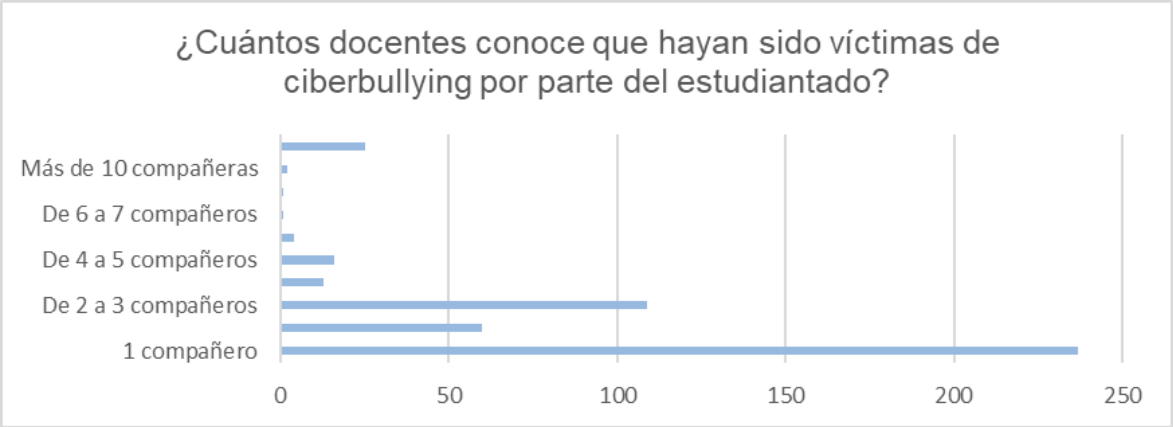
En el ámbito de la percepción de seguridad, la discrepancia entre los docentes que informaron no haber sido víctimas personalmente (82%) y aquellos que conocen casos de ciberataques o ciberbullying hacia los docentes (28.5%) puede indicar que algunos docentes pueden subestimar la prevalencia de estos problemas en su entorno laboral, teniendo implicaciones en la percepción de seguridad y bienestar de los docentes en el lugar de trabajo.

En el nivel de conciencia y sensibilidad se puede decir que el hecho de que una parte significativa de los docentes no estén seguros (10.3% y 9.7% respectivamente) sobre si han sido víctimas o conocen casos de ciberataques o ciberbullying resalta la necesidad de aumentar la conciencia y sensibilidad sobre estos problemas en el entorno educativo.

Los datos sugieren que, si bien la mayoría de los docentes pueden no haber sido directamente afectados por ciberataques o ciberbullying, existe una conciencia generalizada sobre la existencia de estos problemas en el entorno educativo, destacando la importancia de implementar medidas preventivas y de apoyo para garantizar un ambiente de trabajo seguro y saludable para todos los miembros de la comunidad educativa.

Posteriormente se les pidió que continuaran con la siguiente sección aquellos que conocieran casos de ciberataques a los docentes, continuando 467 (48%), es decir, casi la mitad de los encuestados estaban al tanto de casos de ciberataques. Cuando se les preguntó si conocían a alguien que hubiese sido víctima, los datos mostraron que un pequeño porcentaje de docentes conocen a un número considerable de colegas que han sido víctimas de ciberbullying, incluidos casos de más de 10 compañeros o compañeras resaltando la gravedad del problema como se muestra en la Figura 3.

Figura 3. Docentes conocidos que han sufrido ciberbullying.



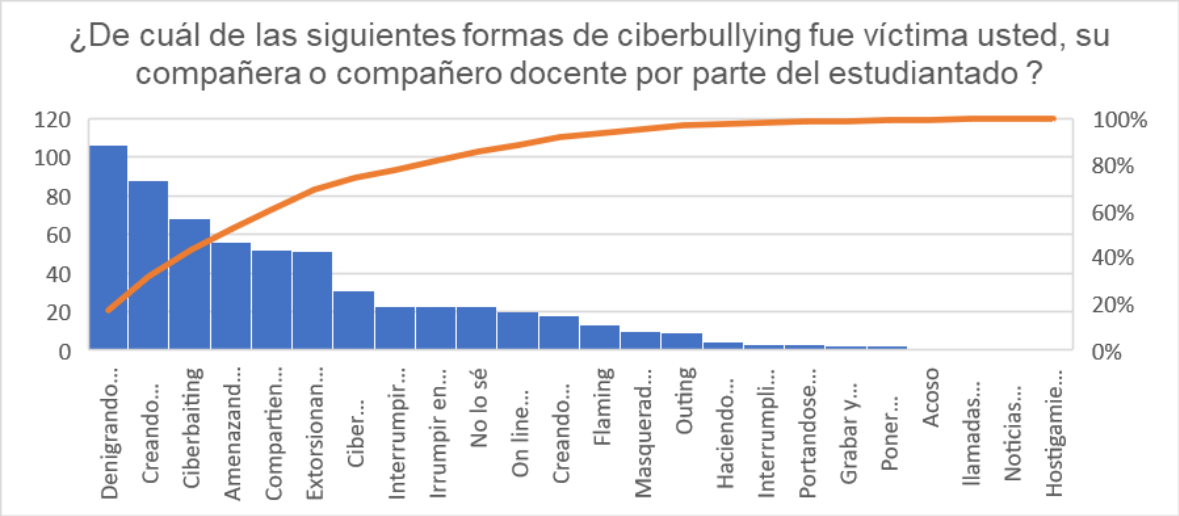
Fuente: Elaboración propia

Los datos muestran que el ciberbullying es una preocupación real dentro del entorno educativo y afecta a un porcentaje significativo de docentes. Se resalta en los datos la frecuencia de víctimas de ciberbullying según el género; mientras que 363 (77%) informaron conocer a compañeros que fueron víctimas, solo 79 (16.9 %) informaron conocer a docentes mujeres.

Se revela una marcada disparidad en la incidencia entre docentes hombres y mujeres. Se puede hablar de la brecha de género, la disparidad en el número de docentes afectados sugiere que los hombres están experimentando un mayor número de casos de ciberviolencia en comparación con las mujeres en este contexto específico, indicando que los hombres son más propensos a ser objeto de ciberataques en este entorno educativo en particular, como lo es el nivel de secundaria. En otro aspecto, es posible que haya diferencias en la forma en que los docentes hombres y mujeres perciben la ciberviolencia. Los hombres podrían ser más propensos a identificar y comunicar los incidentes que experimentan, mientras que las mujeres podrían subreportar, no reconocer ciertos comportamientos, no comentarlos o denunciarlos.

En la pregunta ¿De cuál de las siguientes formas de ciberbullying fue víctima usted, su compañera o compañero docente por parte del estudiantado?, se les pidió que marcaran todas aquellas formas de las cuales, conocían se había llevado a cabo el ciberataque. En la Figura 4 se revela la variedad de formas en que los docentes pueden ser víctimas y resaltan la importancia de abordar adecuadamente este problema y promover un entorno en línea seguro y respetuoso para todos los miembros de la comunidad educativa.

Figura 4. Formas de Ciberbullying del estudiante al docente.



Fuente: Elaboración propia.

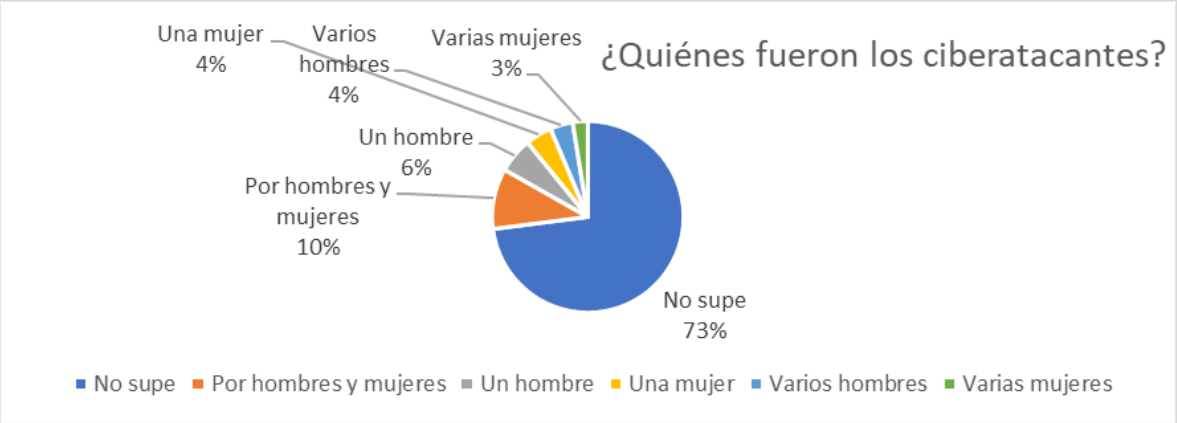
En la Figura 4, se puede observar la frecuencia de cada forma de ciberbullying mencionadas. Las cinco más comunes fueron en primer lugar denigrar publicando historias, fotos o videos dañinos o falsos con 106 casos, en segundo lugar, crear perfiles falsos con 88 casos, en tercer lugar, el ciberbaiting, que implica provocar deliberadamente reacciones

negativas en línea, reportándose 68 casos, en cuarto lugar, las amenazas e intimidaciones en línea o llamadas tuvieron 56 reportes y el quinto fue compartir material degradante, el cual mantuvo un número considerable con 52 reportes.

Cabe aclarar que el sexto lugar lo ocupó extorciones en línea o llamadas con 51 casos y el cuarto amenazas e intimidaciones en línea o llamadas con 56, las cifras indican un problema grave en relación al uso del teléfono celular, la cotidianidad en la práctica docente es la creación de grupos de WhatsApp, haciendo del docente una persona vulnerable ante amenazas, intimidaciones y extorciones.

Cuando se interrogó sobre quiénes fueron los ciberatacantes, los datos mostraron una mayoría que no pudo identificarlos claramente. Sin embargo, también se observa que tanto hombres como mujeres, así como individuos solitarios o grupos, pueden estar involucrados en los ciberataques, como se observa en la Figura 5.

Figura 5. Identificación de los ciberatacantes de los docentes.



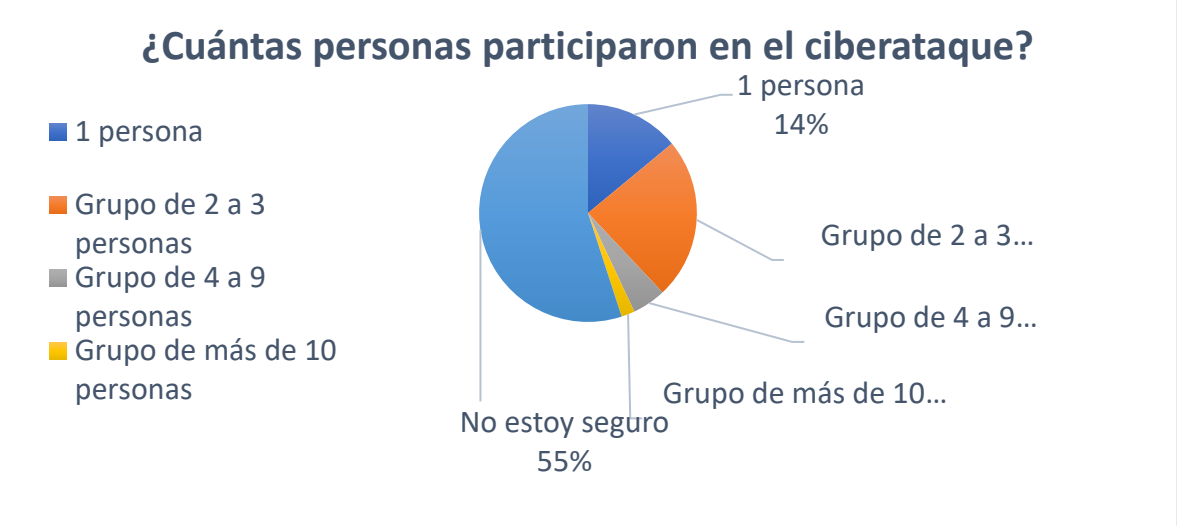
Fuente: Elaboración propia.

La mayoría de los docentes encuestados (343) indicaron que no sabían quiénes fueron los ciberatacantes, lo anterior puede surgir, por haber sido anónimos o difíciles de rastrear. No obstante, el número mayor indica que tanto hombres como mujeres (48 casos) estuvieron involucrados en los ciberataques, un número considerable de casos indicaron que un hombre (28 casos) y una mujer (21 casos) fueron los ciberatacantes, como se puede observar la diferencia en número no es significativa en cuanto a género y en relación a los ciberataques en grupo, la diferencia igualmente no es significativa en cuanto a género, los ataques en grupo se tiene que, varios hombres (18 casos) y varias mujeres (12 casos) estuvieron involucrados.

Dado que los ataques se realizan en medios digitales, es difícil identificar quién o quiénes están involucrados en las infracciones, además, se les cuestionó a los docentes

¿Cuántas personas participaron en los ataques?, la mayoría no logró identificarlos, como se muestra en la Figura 6.

Figura 6. Número de personas que participaron en los ciberataques a docentes.

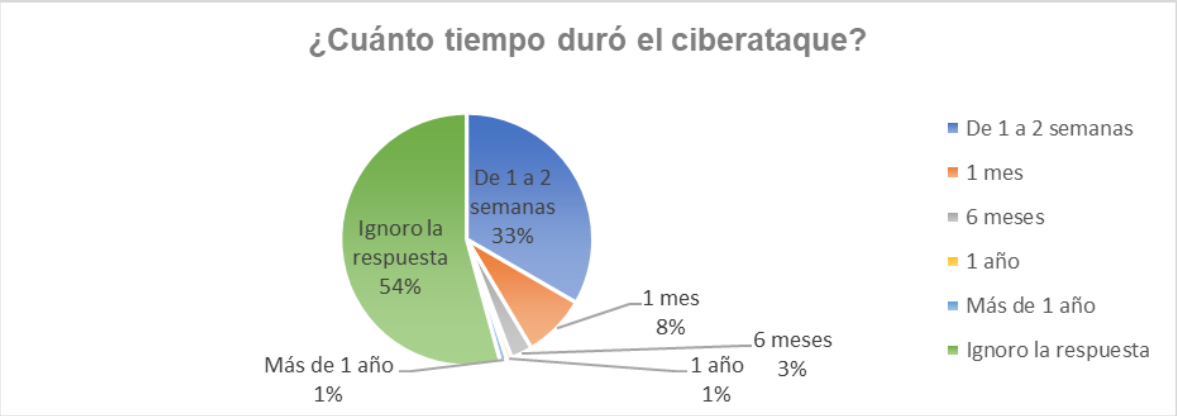


Fuente: Elaboración propia.

La diversidad de los incidentes de ciberataques a los docentes, es proporcional a la distribución de respuestas, dada la gran variedad en la percepción sobre la naturaleza de los ciberataques; mientras que ciertos perciben los ataques como llevados a cabo por grupos de diversas tallas, otros consideran que fueron perpetrados por individuos solitarios.

Cuando se cuestionó sobre el tiempo de duración del ciberataque, los hallazgos obtenidos son preocupantes dado que ciertos casos se llegaron a prolongar durante períodos significativos, como se observa en la Figura 7.

Figura 7. Permanencia del ciberataque.

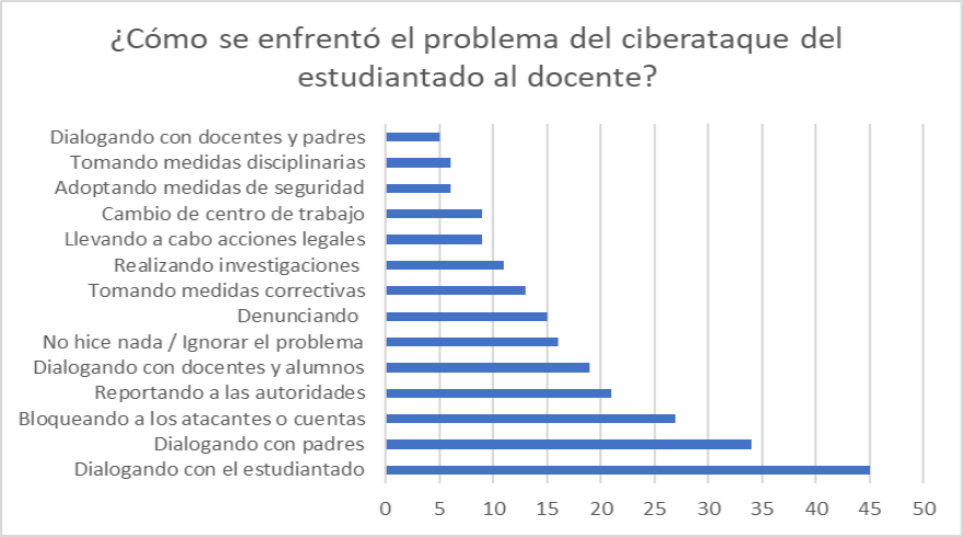


Fuente: Elaboración propia.

Los datos sugieren que los ciberataques dirigidos a los docentes por parte de los estudiantes pueden variar en su duración, desde períodos relativamente cortos hasta situaciones más prolongadas, el hecho de que un número considerable de encuestados indicara que ignoraba la duración del ciberataque resalta la posibilidad de que estos incidentes puedan pasar desapercibidos o no ser plenamente comprendidos por los docentes afectados, además se rescata que, la mayoría de los encuestados indicaron que el ciberataque duró entre una y dos semanas, no obstante, existieron casos que duraron meses o incluso más de un año, lo anterior resalta la gravedad y persistencia de estos problemas.

Los siguientes resultados proporcionan una visión de cómo el docente enfrentó la problemática, revelando una variedad de estrategias utilizadas en el abordaje de ciberataques en el ámbito escolar. En primer lugar, el diálogo, la comunicación directa con el estudiantado surgió como una estrategia fundamental, optado como medida en la resolución personal y directa del problema, evitando involucrar a otros sujetos del contexto educativo, como se muestra en la Figura 8.

Figura 8. Afrontamiento del docente hacia los ciberataques del estudiantado.



Fuente: Elaboración propia.

Las primeras opciones que el docente utiliza para enfrentar el problema son, dialogando con el estudiantado (45), con los padres de familia (34) o bloqueando la cuenta de los atacantes o la suya propia (27) acciones hechas en lo individual, además es preocupante, dar cuenta de que existen docentes que tuvieron que cambiar de centro de trabajo (nueve) o fueron despedidos por ser víctimas de ciberataques por parte del estudiantado (uno), otros casos que no pudieron hacer nada o ignoraron la problemática (16);

no obstante, hubo casos que se comunicaron (21) o denunciaron (21) autoridades escolares. Los hallazgos en su totalidad, subrayan la complejidad y la gravedad de los desafíos que enfrentan los docentes en el contexto de la ciberseguridad escolar.

Discusión

Si bien se ha investigado ampliamente el ciberbullying entre estudiantes, hay una creciente preocupación sobre su impacto en el personal docente, siendo un tema verdaderamente nuevo que poco se ha estudiado.

Las investigaciones de Challenor (2019), Rajbhandari y Rana (2022), así como los datos recopilados en Sinaloa, México, revelan una preocupante tendencia en el aumento del ciberacoso hacia los docentes en distintos contextos geográficos. En la investigación checa, llevada a cabo por Kopecký y Szotkowski (2017), se encontró una prevalencia del 21.73% entre los docentes encuestados, con una muestra que incluía principalmente a docentes de escuelas primarias y secundarias. Contrariamente, el estudio en Sinaloa mostró una mayor prevalencia del 33.7%, con un mayor número de docentes conocedores o víctimas de ciberataques, destacando casos de victimización tanto masculina como femenina. Por otro lado, la investigación de Challenor (2019) en Irlanda reveló una menor prevalencia del 9.5%, indicando que una minoría de docentes de post-primaria había experimentado ciberbullying.

Los hallazgos coinciden en identificar una variedad de formas de ciberataques dirigidos a los profesionales de la educación, que van desde el ciberbaiting y el flaming hasta el ciber-stalking y la creación de perfiles falsos. En las tres investigaciones se documentan casos de acoso en línea, difamación mediante la publicación de contenido dañino o falso, así como amenazas e intimidaciones. La intrusión en cuentas personales y el robo de identidad también son aspectos preocupantes que se destacan en los estudios. Además, se observa una tendencia hacia la interrupción del ambiente educativo, con casos de disruptores que interrumpen clases virtuales con obscenidades y comparten contenido inapropiado en plataformas de mensajería. En particular en Sinaloa las extorciones en línea o llamadas o amenazas e intimidaciones en línea o llamadas son un problema grave debido a la creación de grupos de WhatsApp como parte de la práctica docente.

En el tema del afrontamiento Challenor (2019) identifica estrategias como ignorar el problema y la imposición de límites tecnológicos para proteger su privacidad y restringir el acceso de sus estudiantes a las redes sociales personales, Rajbhandari y Rana (2022) observan una variedad de respuestas que van desde la ignorancia del problema hasta la búsqueda de

apoyo legal y el cambio de trabajo, así como también estrategias de afrontamiento siendo estas la de ignorar el ciberacoso como si no existiera, desactivando sus cuentas en redes sociales y manteniéndose invisibles por un tiempo determinado, dejar el trabajo, tomar acciones legales, buscar apoyo con colegas. En contraste, el estudio en Sinaloa destaca el diálogo como la estrategia principal de afrontamiento, ya sea con los estudiantes, los padres o los propios colegas. Aunque el bloqueo y la denuncia a las autoridades también son comunes, el enfoque inicial se centra en la comunicación y la resolución de conflictos a través del diálogo. Un afrontamiento rescatado por Rajbhandari y Rana (2022) y que no fue optado por los docentes estudiados fue el de mantener registros y pruebas del ciberacoso que estaban experimentando, como una forma de documentar la situación y contar con evidencia en caso de ser necesario para futuras acciones, mismas que deberían implementarse como parte del diario del profesor.

En relación al tiempo que duraron los ciberataques, en el estudio de Challenor (2019) se observó que la duración de los ataques varió considerablemente; se encontró que dos docentes experimentaron ciberataques durante una y dos semanas, mientras que un docente informó que el ataque duró seis meses, y ocho docentes informaron que la duración superó un año. Por otro lado, en Sinaloa, la duración de los ciberataques también fue diversa. Se registraron 156 casos de ataques que duraron de una a dos semanas, 38 casos que duraron un mes, 13 casos con una duración de seis meses, tres casos que se extendieron por un año, y cuatro casos que superaron un año. Además, un número considerable de encuestados (254) indicaron que desconocían la duración de los ataques.

Conclusión

Los datos expuestos a lo largo de esta investigación, proporcionan una visión detallada de la problemática de la ciberviolencia ejercida hacia los docentes en el estado de Sinaloa, así como de las medidas de seguridad utilizadas, las estrategias de afrontamiento empleadas por los afectados y los tipos de perpetradores, evidenciado la necesidad de una mayor conciencia y capacitación sobre ciberseguridad en el ámbito educativo, así como de protocolos y políticas efectivas para abordar la ciberviolencia del estudiantado al docente.

Según los datos encontrados, se destaca la prevalencia de ciberataques y ciberbullying hacia los docentes, con una marcada disparidad en la incidencia entre géneros. Aunque la mayoría de los docentes pueden no haber sido directamente afectados, existe una conciencia generalizada sobre la existencia de estos problemas en el entorno educativo.

En cuanto a las afirmaciones enunciadas en el supuesto de la investigación, se confirma la falta de conocimiento sobre herramientas de seguridad en línea por parte de los docentes, lo que contribuye a su vulnerabilidad ante ataques cibernéticos. En la autoprotección es crucial destacar que, en una primera instancia, los docentes deben ser capaces de autoprotegerse a fin de desempeñar un papel fundamental en la protección de sus estudiantes en el ciberespacio, y es imperativo proporcionarles los recursos y el apoyo necesarios para enfrentar este desafío de manera efectiva. De igual manera, en una primera instancia debe primero saber autoprotegerse, si un docente carece de los conocimientos y habilidades para proteger su propia seguridad en línea, será aún más difícil para él, enseñar eficientemente la ciberseguridad al estudiantado

En relación al vacío de conocimiento, se puede decir que los estudios previos no evaluaron en profundidad la relación entre el conocimiento y el uso de herramientas de seguridad en línea, ni la incidencia de ciberataques según el género de los docentes, lo cual se retoma en este estudio y en este sentido, este trabajo contribuye al campo de la investigación al proporcionar datos empíricos que destacan la necesidad de abordar esta problemática de manera integral y proactiva. Durante la investigación se encontró que algunos docentes no estaban seguros de haber sido víctimas o de conocer casos de ciberataques, lo que sugiere una falta de conciencia o reconocimiento de la problemática. Además, se destaca la necesidad de políticas y medidas específicas para abordar el ciberbullying en el entorno educativo, lo cual es un aporte significativo del presente trabajo.

En esta investigación, se tuvo la limitación de información en cuanto a la falta de seguimiento a largo plazo de los efectos psicológicos en las víctimas, así como las percepciones de los docentes ante los ciberataques y las descripciones de sus experiencias.

Futuras líneas de investigación

De acuerdo a los resultados encontrados, surgen nuevas preguntas de investigación relacionadas a la incidencia de ciberviolencia a los docentes de secundaria en otros estados del país, cuál es su incidencia en otros niveles educativos, cuál es la relación entre el conocimiento y la adopción de medidas de seguridad en línea, cuál es la influencia de factores como la edad y la experiencia en la percepción y respuesta ante la problemática.

Se sugiere realizar un de las víctimas de ciberbullying para evaluar los efectos psicológicos a largo plazo y la efectividad de las estrategias de afrontamiento utilizadas por los docentes afectados. Entre otros estudios se proponen, investigaciones relacionadas a las percepciones de los docentes ante los ciberataques y las experiencias vividas, incluyendo factores como el estrés laboral, la ansiedad y el bienestar emocional.

Se recomienda también diseñar y evaluar protocolos de intervención específicos para abordar el ciberbullying en el entorno educativo, incluyendo medidas preventivas, recursos de apoyo y estrategias de respuesta ante incidentes de ciberviolencia. Por último, investigar la efectividad de políticas y estrategias de prevención del ciberbullying en las escuelas, así como la implementación de programas de educación digital para promover un uso seguro y responsable de la tecnología entre los estudiantes y el personal docente, sería crucial para abordar este problema creciente en el ámbito educativo.

Referencias

Challenor, L. P. (2019). *The Cyberbullying of Post-Primary Teachers in Ireland* [Doctoral dissertation]. Institute of Education, Dublin City University. https://doras.dcu.ie/23733/1/Liam%20Challenor%20PhD%20DORAS%20Copy.pdf

Corral, Y. (2009). Validez y confiabilidad de los instrumentos de investigación para la recolección de datos. *Revista Ciencias de la Educación, 19*(33), 228-247. https://bit.ly/3HcZjOA

Dehue, F., Koeter, M. W. y Schaufeli, W. B. (2009). Pesten op het werk: de relatie met gezondheid en verzuim en de rol van coping. *Gedrag y Organisatie, 22*(2), 97-117. https://doi.org/10.5117/2009.022.002.001

De Wet, C. (2010). Victims of educator-targeted bullying: A qualitative study. *South African Journal of Education, 30*(2). https://doi.org/10.15700/saje.v30n2a341

Dirección de Estudios de Política Educativa, Dirección General de Planeación, Programación y Estadística Educativa- Secretaría de Educación Pública (DGPPYEE-SEP). (2023). *Atlas de los servicios educativos: Representación cartográfica del acceso y prestación de los servicios educativos en México*. (Primera edición). SEP. https://www.planeacion.sep.gob.mx/Doc/Atlas_estados/0000_Atlas_completo.pdf

Dudovskiy, J. (2022). *The Ultimate Guide to Writing a Dissertation in Business Studies: A Step-by-Step Assistance*. (6th ed.). Research Methodology. https://www.scirp.org/reference/referencespapers?referenceid=3477576

Eden, S., Heiman, T. y Olenik-Shemesh, D. (2013). Teachers' perceptions, beliefs and concerns about cyberbullying. *British Journal of Educational Technology, 44*(6), 1036–1052. https://doi.org/10.1111/j.1467-8535.2012.01363.x

Garrett, L. (2014). The student bullying of teachers: an exploration of the nature of the phenomenon and the ways in which it is experienced by teachers. Aigne, (5) 19-40. https://www.ucc.ie/en/media/electronicjournals/aigne/2014-01/03-Garrett-2014-01-en.pdf

Glasow, P. A. (2005, April). Fundamentals of Survey Research Methodology. *Report No. 25988 of Washington C3 Center, McLean, Virginia: MITRE Department.* Division: Department: W800 W804. https://www.mitre.org/sites/default/files/pdf/05_0638.pdf

González, V. (20 de marzo de 2024). Sufren 60% de los maestros violencia por parte de sus alumnos: especialista. *El Heraldo de Chihuahua.*

https://www.elheraldodechihuahua.com.mx/local/chihuahua/sufren-60-de-los-maestros-violencia-por-parte-de-sus-alumnos-especialista-10064719.html

González Torres, A. y Pereira Hernández, M. L. (2023). Encuesta: ciberviolencia dirigida al docente a través de una examinación de autenticidad por dictamen de árbitros. *Revista Internacional de Investigación en Didáctica de las Ciencias y la Matemática, 13*(26). https://doi.org/10.23913/ride.v13i26.1432

Hernández Oropa, M. (2022). Informe violencia digital. Las sociedades patriarcales creamos víctimas y agresores. Un informe para entender cómo, dónde y quiénes perpetúan de forma sistémica la violencia virtual contra las mujeres y niñas en México. Frente Nacional para la Sororidad y Defensoras Digitales.https://leyolimpia.com.mx/wp-content/uploads/2022/12/FNSDG_Reporte2022_DICIEMBRE2022.pdf

Hinduja, S. y Patchin, J. W. (2008). Cyberbullying: An exploratory analysis of factors related to offending and victimization. *Deviant Behavior, 29*, 129-156. https://doi.org/10.1080/01639620701457816

Hua, T. K., So'od, S. M. M. y Hamid, B. A. (2019). Communicating insults in cyberbullying. *Journal of Media and Communication Research, 11*(3), 91-109. https://fslmjournals.taylors.edu.my/wp-content/uploads/SEARCH/SEARCH-2019-11-3/SEARCH2019-P6-11-3.pdf

Huang, Q., Singh, V. K. y Atrey, P. K. (2014). Cyber Bullying Detection Using Social and Textual Analysis. *Proceedings of the 3rd International Workshop on Socially-Aware Multimedia, Orlando, Florida, USA*. https://doi.org/10.1145/2661126.2661133

Instituto del Derecho de las Telecomunicaciones (IDET). (18 de noviembre de 2022). *México está en riesgo por ciberataques, dice Monreal.* IDET (Ed.). https://www.idet.org.mx/noticias/mexico-esta-en-riesgo-por-ciberataques-dice-monreal

Instituto del Derecho de las Telecomunicaciones (IDET). (18 de octubre de 2021). *Mexicanos, los más preocupados.* IDET (Ed.). https://www.idet.org.mx/noticias/mexicanos-los-mas-preocupados

Instituto del Derecho de las Telecomunicaciones (IDET). (23 de noviembre de 2020). *México: 10 mil ciberataques al mes.* IDET (Ed.). https://www.idet.org.mx/noticias/mexico-10-mil-ciberataques-al-mes/

Instituto del Derecho de las Telecomunicaciones (IDET). (27 de diciembre de 2022a*). Los 6 ciberataques que serán más habituales en 2023.* IDET (Ed.). https://www.idet.org.mx/noticias/los-6-ciberataques-que-seran-mas-habituales-en-2023/

Instituto Nacional de Estadística y Geografía (INEGI). (2023). *Maestros y escuelas por entidad federativa según nivel educativo, ciclos escolares seleccionados de 2000/2001 a 2022/2023* [Datos interactivos]. https://www.inegi.org.mx/app/tabulados/interactivos/?pxq=8c29ddc6-eeca-4dcc-8def-6c3254029f19

James, D. J., Lawlor, M., Courtney, P., Flynn, A., Henry, B. y Murphy, N. (2008). Bullying behaviour in secondary schools: What roles do teachers play? *Child Abuse Review, 17*(3), 160-173. https://doi.org/10.1002/car.1025

Juvonen, J. y Gross, E. F. (2008). Extending the school grounds? Bullying experiences in cyberspace. *Journal of School Health, 78*(9), 496-505. https://doi.org/10.1111/j.1746-1561.2008.00335.x

Kauppi, T. y Pörhölä, M. (2012a). School teachers bullied by their students: Teachers' attributions and how they share their experiences. *Teaching and Teacher Education, 28*(7), 1059-1068. https://doi.org/10.1016/j.tate.2012.05.009

Kauppi, T. y Pörhölä, M. (2012b). Teachers bullied by students: Forms of bullying and perpetrator characteristics. *Violence and Victims, 27*(3), 396-413. https://doi.org/10.1891/0886-6708.27.3.396

Kopecký, K. y Szotkowski, R. (2017). Cyberbullying, cyber aggression and their impact on the victim – The teacher. *Telematics and Informatics, 34*(2), 506-517. https://doi.org/10.1016/j.tele.2016.08.014

Kowalski, R. M., Limber, S. P. y Agatston, P. W. (2012). *Cyberbullying: Bullying in the digital age* (2nd ed.). Wiley Blackwell. https://psycnet.apa.org/record/2012-04615-000

Li, Q. (2007). New bottle but old wine: A research of cyberbullying in schools. *Computers in Human Behavior, 23*(4), 1777-1791. https://doi.org/10.1016/j.chb.2005.10.005

Mohajan, H. K. (2020). Quantitative Research: A Successful Investigation in Natural and Social Sciences. *Journal of Economic Development, Environment and People, 9*(4), 52-79. https://mpra.ub.uni-muenchen.de/105149/

Mooij, T. (2011). Secondary school teachers' personal and school characteristics, experience of violence and perceived violence motives. *Teachers and Teaching: Theory and Practice, 17*(2), 227-253. https://doi.org/10.1080/13540602.2011.539803

Olweus, D. (1993). *Bullying at school: What we know and what we can do*. Blackwell Publishers.

Patchin, J. y Hinduja, S. (2006). Bullies move beyond the schoolyard: A preliminary look at cyberbullying. *Youth Violence and Juvenile Justice, 4*(2), 123-147.

Pereira Hernández, M. L. (2021). El docente de secundaria: Una víctima más de los ciberataques. En *Memoria electrónica del XVI Congreso Nacional de Investigación Educativa.* https://www.comie.org.mx/congreso/memoriaelectronica/v16/doc/1404.pdf

Pereira Hernández, M. L. (2023). Violencia al docente: Una revisión sistémica de la circulación del conocimiento. *Dilemas Contemporáneos: Educación, Política y Valores, 10*(3), Artículo no. 45. https://dilemascontemporaneoseducacionpoliticayvalores.com/index.php/dilemas/article/view/3628

Pereira Hernández, M. L. (2024). *Voces silenciadas: Desvelando la violencia y ciberviolencia hacia docentes en estudios de acceso abierto*. Universidad Tecnológica de Puebla. https://doi.org/10.58299/utp.186

Ramos-Galarza, C. A. (2020). Los alcances de una investigación. *CienciAmérica, 9*(3), 1–6. https://doi.org/10.33210/ca.v9i3.336

Rajbhandari, J. y Rana, K. (2022). Cyberbullying on Social Media: An Analysis of Teachers' Unheard Voices and Coping Strategies in Nepal. *International Journal of Bullying Prevention, 5*, 95-107. https://doi.org/10.1007/s42380-022-00121-1

Rigby, K. (1997). Attitudes and beliefs about bullying among Australian children. Irish *Journal of Psychology, 18*, 202-209.

Slonje, R. y Smith, P. K. (2008). Cyberbullying: Another Main Type of Bullying? *Scandinavian Journal of Psychology, 49*, 147-154. https://doi.org/10.1111/j.1467-9450.2007.00611.x

Smith, P. K. y Sharp, S. (1994). *School Bullying: Insights and Perspectives.* Routledge.

Smith, P. K., Mahdavi, J., Carvalho, M., Fisher, S., Russell, S. y Tippett, N. (2008). Cyberbullying: Its nature and impact in secondary school pupils. *Journal of Child*

Psychology and Psychiatry, 49(4), 376-385. https://doi.org/10.1111/j.1469-7610.2007.01846.x

Tolentino, A. C. (2016). Bullying of a teacher in the workplace: A phenomenological study. *International Journal of Learning and Teaching, 2*(1), 20-27. https://doi.org/10.18178/ijlt.2.1.20-27

Whitney, I. y Smith, P. K. (1993). A survey of the nature and extent of bullying in junior/middle and secondary schools. *Educational Research, 35*(1), 3-25. https://doi.org/10.1080/0013188930350101

Zhao, R., Zhou, A. y Mao, K. (2016). Automatic detection of cyberbullying on social networks based on bullying features. *Proceedings of the 17th international conference on distributed computing and networking*, Singapore. https://doi.org/10.1145/2833312.284956